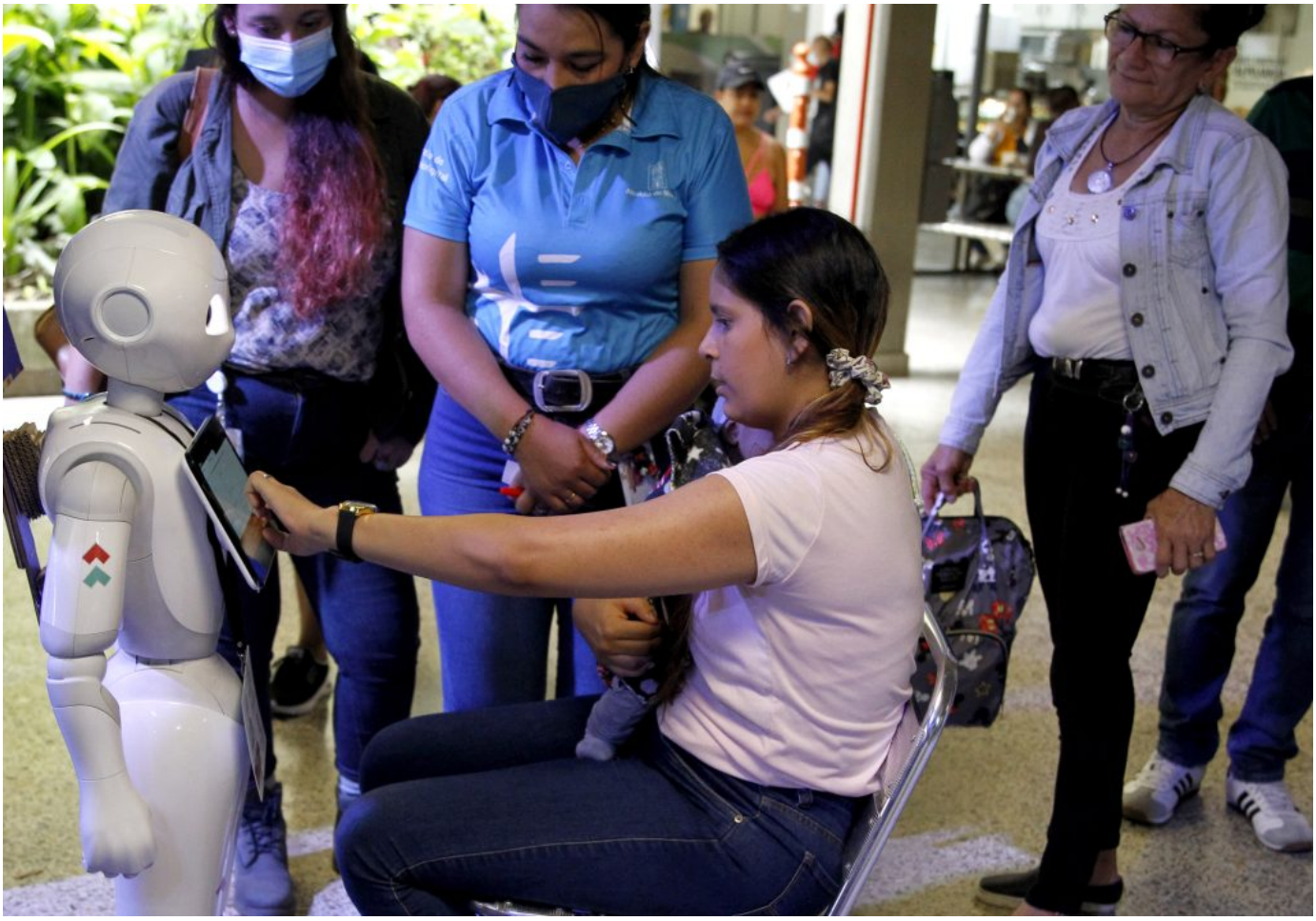
# El futuro del sector tecnológico en Colombia

Mariana Silva Moncayo, Sergio Guzmán



Un asesor guía a los usuarios a interactuar con el robot "Pepper" durante una prueba de los asistentes robóticos Pepper y James en la Alcaldía de Medellín el 08 de julio de 2022 en Medellín, Colombia. (Foto de Fredy Builes/Getty Images)

***La tecnología adquiere cada vez más importancia en la economía colombiana, pero abordar desafíos como la ciberdelincuencia y la escasez de profesionales digitales cualificados deben ser una prioridad para el país si quiere sacar el máximo partido a sus oportunidades.***

Aunque son innegables los beneficios y las oportunidades que la tecnología y la digitalización han proporcionado a Colombia —por ejemplo, la innovación en la búsqueda comercial, productiva y científica y la mayor agilidad de varios procesos productivos e institucionales—, todavía hay factores humanos muy importantes que hacen que sus sistemas sean vulnerables a las amenazas contra la ciberseguridad, el espionaje y las fugas de datos. Estos problemas suponen costes adicionales cuando hay que adaptar y crear unas infraestructuras esenciales

para mitigar los posibles peligros. En la actualidad, Colombia no está manteniendo a las instituciones públicas y privadas muy a salvo de los ciberdelincuentes. El país depende cada vez más de la tecnología, pero paralelamente aumentan los problemas de seguridad que le impiden el pleno desarrollo. Ahora que contempla sacar el espectro 5G a subasta en 2023, Colombia debe abordar estos problemas de seguridad o se enfrentará a desafíos aún más graves en el futuro.

En 2021, Colombia fue el sexto país del mundo que más secuestros de sistemas sufrió, con más de 11 millones de amenazas detectadas. Esta estadística muestra los riesgos que corren las instituciones públicas y privadas y por qué debe ser prioritaria la implantación de protocolos de ciberseguridad. Ante el incremento de los ciberataques y los ciberdelitos, es probable que las empresas aumenten su inversión en infraestructuras de ciberseguridad y sus programas de desarrollo e implementación. En 2021, cuatro entidades estatales colombianas sufrieron ataques informáticos. El Invima y el DANE fueron víctimas de un intento de extorsión y recuperaron el funcionamiento de sus servidores gracias a la ayuda de las autoridades y los equipos técnicos. Las fuerzas militares y la fiscalía fueron víctimas de una filtración del grupo Guacamaya, una organización de activismo informático con fines políticos que está en una campaña permanente para desprestigiar a las empresas del sector extractivo y a las fuerzas armadas de varios países latinoamericanos. En el caso de Colombia, la información filtrada ascendió a más de cinco terabytes de datos (unos 38.000 archivos), con informaciones sobre casos polémicos, como las escuchas telefónicas del Ejército y la Policía, el caso Odebrecht e Iván Márquez y Jesús Santrich, entre otros. Mientras la opinión pública siga pensando que hay una injerencia de las empresas en la política, la reputación de las firmas que quieran hacer contribuciones —aunque sean legales— a campañas electorales o partidos políticos estará en peligro.

Las entidades estatales, tanto nacionales como locales, necesitan mejorar e instaurar protocolos e iniciativas de políticas públicas sobre ciberseguridad. Sobre todo, porque muchos fiscales de Latinoamérica no tienen la formación necesaria para abordar estos delitos. La complejidad de la ciberdelincuencia y su continua evolución significan que probablemente la ley va a ir siempre por detrás. Los ataques contra informaciones críticas y confidenciales dejan claro que ninguna institución está a salvo y ponen de manifiesto las preocupantes vulnerabilidades cibernéticas del país. Y además indican que las inversiones en ciberseguridad son insuficientes. Si no se instauran nuevos protocolos o se actualizan las leyes y normas digitales, seguramente los ciberdelitos serán cada vez más frecuentes y afectarán a las entidades en cuestión y a otros actores relacionados con ellas.

El Decreto 338 de 2022 es el más reciente intento normativo de reforzar la reacción del

Gobierno frente a la ciberdelincuencia. Permite a las entidades públicas prevenir y gestionar los riesgos de incidentes cibernéticos, mejorar la gobernanza de la seguridad digital e identificar las infraestructuras informáticas críticas. Asimismo oficializa el radio de acción de los Equipos de Respuesta a Incidentes Cibernéticos (como ColCERT y CSIRT), que son los organismos gubernamentales encargados de la ciberseguridad nacional. A pesar de estos avances, el país tiene un marco legal débil y una formación escasa en gestión e investigación de delitos informáticos, además de insuficiente experiencia institucional a la hora de denunciar incidentes. Esto hace que quienes comunican informaciones privadas a las entidades gubernamentales afectadas corran riesgos como la falta de disponibilidad de servicio, pausas operativas y pérdidas económicas.

**Desafíos en el horizonte**

El incremento de la piratería informática y los ataques hará que la protección de datos sea una prioridad para las empresas. Por consiguiente, aumentará la demanda de programas de ciberseguridad y, con ella, la demanda de informáticos, codificadores e ingenieros de *software* colombianos, cuyo talento y capacidad de innovación, según Procolombia, gozan de reconocimiento internacional. El sector está creciendo en Colombia, gracias a un importante esfuerzo del Gobierno anterior para convertir el país en el "Silicon Valley de Latinoamérica", que derivó en más inversiones extranjeras directas en el sector y más exportaciones relacionadas con la tecnología. En 2021, el Ministerio de Comercio registró unas exportaciones de *software* y servicios informáticos por valor de 218,8 millones de dólares, un 33% más que en 2020, con Uruguay, Estados Unidos, Panamá, México y Costa Rica como principales compradores, lo que indica que ha crecido en los últimos dos años.

A pesar de algunas señales alentadoras, Colombia sigue sufriendo una escasez cada vez mayor de profesionales digitales cualificados. En la actualidad faltan alrededor de 80.000 empleados y, según cálculos del MinTic, para 2025 el país tendrá un déficit de talento digital de entre 68.000 y 112.000 desarrolladores de *software.* El Gobierno y el sector privado tendrán que resolver cómo formar y promocionar a profesionales para cubrir la demanda creciente de servicios informáticos a corto plazo. Dado que es un sector que necesita un enorme capital humano, esta es además una oportunidad de creación de empleo que el gobierno de Gustavo Petro no puede pasar por alto.

Una de las nuevas tareas del nuevo Ejecutivo es sacar a subasta las redes 5G de Colombia en el primer semestre de 2023. La licitación será algo más que un simple concurso de contratos, puesto que China y Estados Unidos se disputan ferozmente en el escenario mundial el control de la banda ancha digital. EE UU ve con malos ojos que Colombia adjudique la licitación a

Huawei o ZTE, ambas con presencia en Colombia y sancionadas por las autoridades estadounidenses y europeas. Si el gobierno de Petro no se aclara cuanto antes en materia digital, o Estados Unidos o China podrá aprovechar en beneficio propio las vulnerabilidades digitales del país.

En resumen, el sector tecnológico ha adquirido cada vez más importancia en la economía colombiana. Sin embargo, nuestro análisis da a entender que existen muchas posibilidades de crecimiento y desarrollo, pero también muchos obstáculos que impiden que Colombia saque el máximo partido de esas oportunidades. Tanto las posibilidades cada vez mayores del sector de la informática y las tecnologías de la información como la importancia creciente de la ciberseguridad no son más que dos ejemplos de los beneficios que podría obtener Colombia. El país tendrá que dar un paso más para mitigar o reducir su vulnerabilidad digital. Para lograr un entorno virtual que sea seguro para los ciudadanos y las empresas, tanto el sector privado como el público tendrán que esforzarse en sacar adelante nuevos proyectos legislativos que aborden la enorme complejidad de la ciberdelincuencia y el peligro de lagunas legales a la hora de perseguir a quienes cometen esos delitos.

*Esta versión original fue publicada en Global Americans. Traducción de María Luisa Rodríguez Tapia.*

**Fecha de creación**
16 diciembre, 2022